Conclusions on the joint inspection of the supervisory authorities of the Baltic States on the compliance of personal data processing in the field of short-term vehicle rental

I. GENERAL INFORMATION

The supervisory authorities of the Baltic States (Data Protection Inspectorate of Lithuania, Data State Inspectorate of Latvia, State Data Protection Inspectorate of Estonia, hereinafter referred to as the Supervisory Authorities or Authorities) agreed to perform a preventive inspection on the compliance of personal data processing in the field of short-term vehicle rental.

The Supervisory Authorities carried out a preventive inspection in the field of short-term vehicle rental services in order to find out whether short-term vehicle rental service providers, which are established and operate in Estonia, Latvia and Lithuania and provides short-term vehicle rental services to natural persons in the Baltic States, comply with the provisions of the Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to personal data processing and free movement of such data and which repeals the provisions of Directive 95/46 EC (General Data Protection Regulation) (hereinafter - GDPR).

The implementation of coordinated monitoring measures results from the 2021 meeting of Supervisory Authorities, during which the Authorities agreed that in 2022/2023 - in Estonia, Latvia and Lithuania, sectoral monitoring will be organized, with the aim of developing recommendations for improving personal data processing and protection processes, in a pre-agreed sector.

The Authorities agreed on criteria of the service providers, who were selected for the inspection:

- ✓ Those who offer short-term rental (car-sharing) of vehicles, including electric scooters;
- ✓ The main recipient of services is a natural person;
- ✓ Place of activity – Baltic states.

II. SCOPE OF THE INSPECTION

All Supervisory Authorities take into account at least some of the criteria mentioned below, while maintaining the responsibility of each supervisory authority to take into account other aspects in the selection of the target audience, maintaining the main inspection framework (processing of personal data, providing short-term vehicle rental services to natural persons, compliance with the GDPR):

- ✓ Enterprises providing services in all Baltic States and such Enterprises providing services in at least two Baltic States.
- ✓ Enterprises whose controller or joint controller (persons responsible for the protection of personal data defined in Article 4 (7), (8) of the GDPR) are located in one of the Baltic States (the inspection of the specific enterprises is initiated by the country where the main establishment is situated);
- ✓ Enterprises on which activities' (compared to others in the same market) most complaints/applications are submitted;
- ✓ Enterprises that occupy the majority of the market of vehicle rental services;
- ✓ Enterprises that are (partially) financed by consumers (Tuul Mobility OÜ has publicly issued bonds);
- ✓ Enterprises known for their use of large-scale consumer-oriented advertising.

Considering the mentioned criteria, the Supervisory Authorities chose eight enterprises that provide short-term vehicle rental services in the territories of the Baltic States (hereinafter – Enterprises):

1. Ltd. TRANSPORT (SIXT);
2. Ltd. SLYFOX (CARGURU);
3. Ltd. RIDE;
4. SIA "ETERNA ELECT" (Skok);
5. UAB "Prime leasing" (CityBee).
6. Bolt Operations OÜ;
7. ELMO Rent AS (the monitored services have been terminated by the time the report is completed);
8. Tuul Mobility OÜ.

As part of the inspection, it was assessed whether the personal data that Enterprises process in order to provide the vehicle rental service:

- ✓ is adequate (Article 5 (1) (c) of the GDPR);
- ✓ is processed according to the purpose (Article 5 (1) (b) of the GDPR);
- ✓ complies with the storage limitation principle (Article 5 (1) (e) of the GDPR);
- ✓ has appropriate legal basis of the processing (Article 6 of the GDPR).

By carrying out coordinated monitoring activities in the home countries of the Supervisory authorities, the Supervisory Authorities have come to relatively similar conclusions regarding the inconsistencies in the processing of personal data of Enterprises in the field of short-term vehicle rental, which can be found in the section below.

III. CONCLUSIONS OF THE INSPECTION

1. **Determination of the appropriate legal basis.**

One of the most significant inconsistencies found in the processing of personal data of vehicle rental service providers is the inappropriate choice of legal basis or the inability to sufficiently justify the choices made. Sometimes the legal basis of the processing and the amount of processed personal data specified in the privacy policy (data processing regulations) differed from what the Enterprises provided in their responses to the Supervisory Authorities. There have also been cases where one legal basis is specified for all processing operations, including processing operations for which this legal basis is not applicable.

The legal basis for the processing of personal data, which the Enterprises relied on the most, is the performance of a contract to which the data subject is a party, or the need to take measures before concluding the contract (Article 6 (1) (b) of the GDPR). This legal basis was also used for personal data processing that is not necessary for the performance of the contract. For some processing the correct legal basis would be legitimate interests (Article 6 (1) (f) of the GDPR). As a result of incorrect determination of the legal basis, some of the Enterprises have not carried out a legitimate interest balancing test which is required by Article 6 (1) (f) of the GDPR.

2. **Data volume.**

Although the scope of requested personal data varies from customer to customer, the

overall amount of information that Enterprises need in order to provide service to customers is similar. Some Enterprises do not request separately any specific information from the customer thus requesting smaller amount of data as an obligatory filled information, for example, do not request social security number or date of birth. However, the mentioned information is obtained in an indirect way, for example, by asking to send a driver's licenses photo, which contains above mentioned data.

In some cases, the amount of personal data requested from the person, when they want to get service and have to submit the request, differs from the amount of data necessary to get the service defined in the privacy policies on Enterprises websites.

3. Transparency.

A lack of compliance with the principle of transparency was identified in a number of enterprises in the form of a failure to provide meaningful information to data subjects. It was detected that:

- ✓ Enterprise's privacy policy and terms of service do not include all the information on personal data processing contained in Chapter III of the GDPR;
- ✓ Neither the Enterprise's privacy policy nor the terms of service specify when the customer's documents confirming the right to drive are / may be checked, in order to verify the validity of the customer's driver's license;
- ✓ During the investigation it was found that Enterprises distinguishes "suspicious" customers in the records of processing, but information about the classification of customers as "suspicious" is not provided either in the privacy policy, nor in Enterprise's terms of service. In certain situations, the information provided to the supervisory authority was incomplete and did not match the information published in Enterprise's privacy policy and terms of service.

4. Retention periods.

Although in most cases no inconsistencies in the processing of personal data were found in this aspect, in some cases the storage periods indicated by the Enterprises were definitely too vague (for example, the data is stored for as long as it is necessary or permitted under the applicable law, or to achieve the objectives specified in the privacy statement goals). Therefore, from the set of answers and publicly available information, it is not clear how long and for what reasons certain types of data are stored. In some Enterprises, inconsistencies in technical requirements were found, which to some extent is related to the storage period. Namely,

customers' personal data were not deleted under certain and identified conditions. Although the non-conformity has been eliminated, such situations would not happen if Enterprise had taken all the necessary technical measures to ensure data processing compliance in a timely manner, including periodic review of processing activities.

5. Biometric data

Considering the answers provided by the Enterprises, it can be concluded that in most cases the identification of customers, as well as further processing of personal data, takes place without the use of biometric data. However, in some cases, in order to confirm identity, customer facial image data (among other data) is processed based on data subjects' consent (Article 9 (2) (a) of the GDPR). In order to comply with the requirements of Article 7 of the GDPR and to ensure that consent is given freely and the data subject has choices regarding the provision of consent, Enterprises include information in the privacy policy about the option not to use biometric data, i.e. customers can contact Enterprise who can offer an alternative for biometric data. However, neither Enterprise's terms of service nor the privacy policy provides customers with an equivalent, freely chosen identified alternative that allows to not use biometric data.

VI. RECOMMENDATIONS

1. Determination of the appropriate legal basis.

Article 6(1)(b) of the GDPR must be interpreted strictly and in a narrower manner. It is not applicable in cases where the processing is not necessary to fulfill the contract but is unilaterally determined by Enterprise to fulfill the enterprise's interests. Furthermore, the fact that part of the data processing is covered by a contract does not mean that such processing is necessary for its performance. For example, Article 6(1)(b) is not a suitable legal basis for customer profiling or sending commercial communications. Even if such processing activities are specifically indicated in the fine print of the contract, this does not mean that data processing is "necessary" for the performance of the contract.

On the other hand, in cases where the processing is not considered necessary for the performance of the contract and the service can be provided without carrying out the specific processing, another legal basis should be determined. Enterprises after the evaluation of the nature of each processing can

use other legal basis prescribed at the GDPR, for example, legitimate interests (Article 6 (1)(f)) or consent (Article 6 (1) (a)), as long as the relevant conditions are met.

Article 6(1)(f) of the GDPR (processing is necessary for the legitimate interests of the controller or a third party, except when the interests of the data subject or fundamental rights and fundamental freedoms that require the protection of personal data are more important than such interests, in particular if the data subject is a child) covers situations where the processing indirectly related to the performance of a contract to which the data subject is a contracting party.

In the context of vehicle rental, this could be the processing of vehicle location (GPS), data for fleet monitoring and theft prevention. However, the use of GPS is subject to a different legal basis depending on the purpose of data processing. For example, 6 (1) (b) of the GDPR could be applicable to find out the identity of the customer who has committed a violation of the Road Traffic Regulations and as a result has violated the contract. Article 6 (1) (c) of the GDPR also refers to Enterprise's obligation to report personal data in the event of an administrative violation. And the use of GPS in the customer's device falls under 6 (1) (a), if the purpose of the data processing is to provide the customer with accurate distances from his location to the vehicle.

In the case of processing customers' biometric data on the grounds of consent, elements of valid consent must be taken into account[1]. 'Consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her (Article 4 (11) of the GDPR). Among other things, it is to be noted that the element "free" implies real choice and control for data subjects. As a general rule, the GDPR prescribes that if the data subject has no real choice, feels compelled to consent or will endure negative consequences if they do not consent, then consent will not be valid[2]. It should be noted that to ensure the voluntariness of consent, the data controller should provide an alternative, not overly burdensome, method of identity verification.

The table below summarizes the most frequently found personal data and the purposes of personal data processing and their possible legal bases. Please note that each situation must be evaluated individually and the most suitable legal basis may differ in different circumstances.

[1] See European Data Protection Board Guidelines 05/2020 on consent under Regulation 2016/679
[2] See European Data Protection Board Guidelines 05/2020 on consent under Regulation 2016/679 recital 13

Personal data	Legal basis (Article 6 of the GDPR)
Personal identification data (name, surname, personal code / identification number, date of birth), facial image (biometric data)	Article 6 (1) (b) - to identify the identity of a person in order to conclude a contract Article 9 (2) (a) - use of the face recognition tool
Location data (GPS data)	Article 6 (1) (f) Monitoring of the car park, prevention of theft Article 6 (1) (b) To establish the identity of the customer who committed the violation of road traffic rules and, as a result, has breached the contract Article 6 (1) (c) Obligation to report personal data in the event of an administrative offense Article 6 (1) (a) To provide the client with accurate distances from his/ her location to the vehicles
Postal address of residence (city, street, house no., apartment no.)	Article 6 (1) (b) To send the official notices
Contact information (phone number, email address)	Article 6 (1) (b) For communication, related to contract performance (e.g., to inform about new available vehicles, changes in payment policy, etc.) Article 6 (1) (f) For communication to reduce the number of traffic accidents due to speeding (automated calls to customers who exceed the speed limit) Article 6 (1) (a) Sending commercial communications
Driver's license details (photo, license number, expiration date, current driving license categories)	Article 6 (1) (b) To check the person's right to drive a vehicle and the current categories of driving rights in force
Information on received administrative violations	Article 6 (1) (b), (c) and (f) For the protection of interests and the management of the terms of the contract
Information about the concluded contract (term concluded, selected service, conditions)	Article 6 (1) (b) For the control and management of contractual relations providing the service and after it’s end in

	relation to situations that may occur after the end of the period of service
Information about traffic accidents	Article 6 (1) (f) For protection of interests, evaluation of accidents, improvement of service quality, insurance compensation application
Billing/Payment Data Name, surname, card number, expiration date and CVC number of the cardholder	Article 6 (1) (b) To receive payment of the provided service Article 6 (1) (c) To ensure payment flow

2. Volume of data

Data minimization should be carried out at an early stage of personal data processing, without collecting data that can be dispensed with. It is necessary to implement the determined goal with the minimum amount of data necessary for its achievement. This means that no more data than is necessary to provide the service may be collected.

To determine the appropriate amount of data, the following points should be taken into account:

- ✓ Personal data that are processed must be adequate and not excessive, taking into account the purposes for which they are processed;
- ✓ Certain data entry fields should be developed in such way that they would not provide redundant space for entering data that is not necessary;
- ✓ Unnecessary personal data must be deleted after the specified time;
- ✓ Periodic checks regarding the amount of personal data to be processed, its necessity have to be carried out.

3. Transparency

Taking into account the principle of transparency established in the GDPR, the controller must ensure the processing of personal data that allows the data subject to understand what data, for what purpose and on what legal basis is being processed.

Data subjects must have access to all information about their personal data being collected, used, viewed or otherwise processed and to what extent personal data is or will be processed. The principle of transparency is based on the requirement that all information and communication related to said processing of personal data is easily accessible and easy to understand and that clear and simple language must be used. Said principle applies in particular to information to data subjects about the identity of the controller and the purposes of the processing, as well as additional information to ensure

fair and transparent processing for the natural persons concerned, and their right to receive confirmation and notification of which of their personal data is being processed. Individuals should be informed about the risks, rules, safeguards and rights related to the processing of personal data and how to exercise their rights related to such processing.

In order to implement the principle of transparency in accordance with the requirements of the GDPR, the controller must perform the following actions:

- ✓ Information about the processing of personal data must be easily accessible and easily understood by the user in clear and simple language. The information must be available in the national language of the respective country where the controller operates. If there are several, then in all national languages. If the administrator operates in several countries, then the information must be available in the national language of each country;
- ✓ The information specified in the privacy policy must correspond to the processing carried out in practice by the controller regarding the amount of personal data, purposes, legal bases. The information that is specified in the privacy policy must reflect the practical behavior of the controller and the actions taken with the data. If the processing activities change, the privacy policy must be changed accordingly.
- ✓ In the privacy policy, such information should be specified that would fully allow the data subject to understand who the controller is, what data are processed, what are the purposes of processing and the legal basis, in which way the data subject can exercise their rights. Basic information should be as follows:
    - ➢ enterprise's name and contact information;
    - ➢ contact information of the data protection specialist (the e-mail address must be specified, where the controller can be contacted with questions about data protection or with a data subject data access request);
    - ➢ purpose of processing;
    - ➢ types of data processed;
    - ➢ the legal basis of processing (one of the legal grounds of Article 6 (1) of the GDPR);
    - ➢ source of data collection;
    - ➢ data recipients or their categories;
    - ➢ data retention period/requirements;
    - ➢ whether the data is sent to third countries or international organizations;
    - ➢ instructions on how to delete personal data.

- ✓ The information in the privacy policy must be updated regularly, it must correspond to the enterprise's current processing of personal data;
- ✓ The privacy policy should be posted on the website or app in an easily accessible location.

4. Data retention period

Each period of personal data processing should be clear, legitimate and determined already at the time of personal data collection. It would be necessary to evaluate the duration of data storage, ensuring that the storage period of personal data is strictly limited to a minimum. Personal data should contain only what is necessary for the purposes for which it is processed. In order to be able to identify data processing inconsistencies in a timely manner, enterprises should periodically review the relevance of their internal data processing policies to processing activities. This is especially important in cases where processing operations have occurred or processing for a new purpose has begun. The same applies to technical measures, that is, their adequacy should be periodically reviewed taking into account the current progress of available technologies.

Similarly, annual training of employees in the field of personal data processing is no less important. A qualified and knowledgeable employee will be able to identify data processing inconsistencies in time and eliminate them. In addition, regular employee training will help employees to comply with the principles of personal data processing in their work, which will allow entrepreneurs to avoid financial and/or reputational losses in the long run.

In order to implement the principle of storage in accordance with the requirements of the GDPR, the controller must perform the following actions:

- ✓ personal data should not be stored longer than is necessary for the purposes for which they are processed;
- ✓ appropriate mechanisms (rules, procedures) for automatic deletion of personal data must be established;
- ✓ if this is not possible and the data is deleted manually, periodic checks should be carried out on compliance with the data deletion deadlines;
- ✓ periodic review of the terms / necessity of personal data storage (maximum period);
- ✓ annual training of employees in the field of personal data processing must be provided;
- ✓ a periodic review of security settings and access rights must be carried out;
- ✓ clear and understandable retention periods must be established. If the storage term is defined in the regulatory act, then the specific term must be indicated in the privacy policy.

5. Biometric data

When using the customer's special category data (face image data), the controller must not only rely on one of the legal bases of Article 6 of the GDPR, but also rely on one of the exceptions to the prohibition of processing special category data set out in Article 9 of the GDPR.

The use of biometric data (face image data) by Enterprises is legally possible only with the provision of appropriate explicit consent. Explicit consent is one of the exceptions to the prohibition of processing special categories of data. However, for the consent given by the data subject to be valid, it must comply with the provisions of Article 7 of the GDPR. This means that consent must be:

- ✓ freely given
- ✓ for a specific purpose
- ✓ intentional and informed
- ✓ an unambiguous indication of the wishes of the data subject, with which he gives his consent to the processing of his personal data in the form of a clear affirmative action.

Data subjects should have real choice and control over their data. In cases where the data subject has no real choice, where he feels that the consent is coerced or that not giving it will result in adverse consequences, the consent will not be valid. Where consent is included as a non-negotiable part of the terms, it is not freely given.

Therefore, Enterprises must be able to ensure that consent is given freely and there is a real alternative that can be used in cases where the data subject does not want to give his consent or has withdrawn it. As an example of an alternative use of biometric data, the Institutions consider face-to-face document verification or video call verification.

The authorities do not rule out other alternatives, however, they emphasize that in these cases it is important to ensure that it does not create an excessively large administrative or other burden, thus influencing the data subject to give his consent.